REMARKS

Applicant respectfully requests allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1-39 are pending in the application, with claims 1, 13, 23 and 28 being independent. Claims 1, 13, 23 and 28 are amended. Claims 3, 5, 6, 12, 15, 17, 18, 26, 27, 30, 32 and 33 are canceled. Support for claim amendments and additions can be found in the original disclosure at least in dependent claims 3, 5, 6, 12, 15, 17, 18, 26, 27, 30, 32 and 33.

Claim Rejections under §101

Claims 28-39 are rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter. In particular, the Office states that the "medium" includes signals. For the sole purpose of expediting allowance and without conceding the propriety of the Office's rejections, the specification is amended as shown above.

Accordingly, the Applicant respectfully requests that the Patent Office withdraw the rejections under 35 U.S.C. § 101.

§§ 102 and 103 Rejections

Claims 1, 2, 4, 8, 10, 13, 14, 16, 20, 23-25, 28, 29, 31, 36, and 38 are rejected under 35 U.S.C §102(e) as being anticipated by U.S. Patent Application No. 2003/0081771 A1 (hereinafter "Futa").

Claims 1-5, 7-17, 19-26, 28-32 and 34-39 are rejected under 35 U.S.C. §102(a) as being anticipated by NPL, Anonymous, November 2003 (hereinafter "Anonymous").

Claims 3, 7, 15, 19 and 34 are rejected under 35 U.S.C. §103(a) as being obvious over Futa in view of NPL, Katsura 1975 (hereinafter "Katsura").

Claims 5, 9, 11, 17, 21, 22, 26, 35 and 39 are rejected under 35 U.S.C. §103(a) as being obvious over Futa in view of U.S. Patent No. 7,113,594 (hereinafter "Boneh").

Claims 6, 18, 27 and 33 are rejected under 35 U.S.C. §103(a) as being obvious over Futa in view of Boneh and further in view of NPL, Eisentrager November 2003 (hereinafter "Eisentrager").

Claims 12 and 37 are rejected under 35 U.S.C §103(a) as being obvious over Futa in view of Katsura.

Applicant respectfully traverses the rejections. Nevertheless, for the sole purpose of expediting allowance and without conceding the propriety of the Office's rejections, Applicant has revised independent claims 1, 13, 23 and 28.

Independent claim 1, as amended, recites a method comprising:

- generating an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular

generation, linearly independent generation, and combinations thereof;

- publishing a public key corresponding to the isogeny;
- encrypting a message using a encryption key corresponding to the isogeny; and
- decrypting the encrypted message using a decryption key corresponding to the isogeny, wherein the decrypting is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing; and
- using a trace map to shorten points on an Abelian variety.

The Office argues that Futa anticipates the subject matter of claim 1 (prior to the amendment to this claim). Applicant respectfully disagrees. Nevertheless, without conceding the propriety of the rejection and in the interests of expediting allowance of the application, independent claim 1 is amended to recite that the "isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof." Independent claim 1 is further amended to recite that "the decrypting is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing." Finally, independent claim 1 is amended to recite

that the method comprises "using a trace map to shorten points on an Abelian variety." Dependent claims 3, 5, 6 and 12 are incorporated into claim 1 with this amendment. Claim 3 is rejected under 35 U.S.C. §103(a) as obvious over Futa in view of Katsura and is also rejected under 35 U.S.C. §102(a) as being anticipated by Anonymous. Claim 5 is rejected under 35 U.S.C. §103(a) as obvious over Futa in view of Boneh. Claim 6 is rejected under 35 U.S.C. §103(a) as being obvious over Futa in view of Boneh and in further view of Eisentrager and is also rejected under 35 U.S.C. §103(a) as being obvious over Anonymous in view of Eisentrager. Claim 12 is rejected under 35 U.S.C. §102(a) as being anticipated by Anonymous.

Applicant respectfully submits that neither Futa, Katsura, Anonymous, or a combination thereof teaches or suggests incorporated **dependent claim 3**.

First, Applicant respectfully submits that the cited reference Anonymous, published November 3, 2003 does not constitute prior art. The current application, 10/816,083 claims priority of a provisional application, 60/517,142, filed on November 3, 2003. The cited reference Anonymous was published on the same day and therefore, cannot constitute prior art. Accordingly, Applicant requests that the §102(a) rejection with respect to dependent claim 3, prior to amendment, be withdrawn.

Futa, meanwhile, is directed to "an elliptic curve converting device that converts a first elliptic curve defined on a finite field F into a second elliptic curve defined on the finite filed F." (Futa, Abstract) Futa recites that "[t]o seek the

elliptic curve that is an isogeny of degree L of the elliptic curve E, a modular polynomial can be used." (Futa, Paragraph [0154])

However, Futa fails to teach "a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof" as recited in amended claim 1. Further, Futa fails to teach that the "decrypting is performed by bilinear pairing[,] wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing."

Katsura, meanwhile, is directed to theorems on the structure of singular Abelian varieties. Katsura is cited for its alleged teaching of "generating isogenies using complex multiplication, linearly independent generation and combinations thereof." However, similar to Futa, Katsura fails to teach "decrypting is performed by bilinear pairing[,] wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing."

Thus, claim 3 as incorporated into independent claim 1 is allowable over Futa and Katsura, whether taken alone or in combination (assuming for the sake of argument that the documents can even be combined).

Furthermore, Applicant respectfully submits that neither Futa, Boneh, or a combination thereof teaches or suggests incorporated **dependent claim 5**. In making out a rejection of this claim, the Office cites to Anonymous. For the reasons described above, Applicant respectfully requests that the rejection be withdrawn, as Anonymous does not meet the requirements to be cited as prior art.

In making out a further rejection of this claim, the Office cites to Futa as teaching "decrypting is performed by bilinear pairing." Applicant respectfully disagrees.

As stated above, Futa is directed to "an elliptic curve converting device that converts a first elliptic curve defined on a finite field F into a second elliptic curve defined on the finite filed F." (Futa, Abstract)

However, Futa does not teach that "the decrypting is performed by bilinear pairing." Futa also fails to teach "a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof" as recited in amended claim 1. Further, Futa fails to teach that the "decrypting is performed by bilinear pairing[,] wherein the bilinear pairing paring is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing."

Boneh, meanwhile, is directed to "[a] method and system for encrypting a first piece of information M to be sent by a sender [100] to a receiver [110] [which] allows both sender and receiver to compute a secret message key using identity-based information and a bilinear map." (Boneh, Abstract) Boneh recites that "[a]n embodiment of the invention is directed to a method of decrypting ciphertext…[a]t least a portion of the ciphertext is dexrypted using a bilinear map and the decryption key." (Boneh, Column 3, lines 4-12). However, Boneh does not teach that "the *isogeny* is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly

independent generation, and combinations." (Emphasis added.) Boneh also does not teach "using a trace map to shorten points on an Abelian variety."

Thus, claim 5, as incorporated in claim 1 with its additional recitations as discussed above, is allowable over Futa and Boneh, whether taken alone or in combination (assuming for the sake of argument that the documents can even be combined).

Applicant respectfully submits that neither Futa, Boneh, Eisentrager or Anonymous or a combination thereof teaches or suggests incorporated **dependent claim 6**. In making out a rejection of this claim, the Office cites to Eisentrager and Anonymous. For the reasons described above, Applicant respectfully requests that the rejection be withdrawn since Eisentrager and Anonymous do not meet the requirements to be cited as prior art. Consequently, Applicant respectfully submits that the two §103(a) rejections be withdrawn with respect to dependent claim 6 since both rejections are based on references that do not constitute prior art for the subject application.

Applicant respectfully submits that **dependent claim 12** is allowable. In making out a rejection of this claim, the Office cites to Anonymous under §102(a). For the reasons stated above, Applicant respectfully submits that this rejection be withdrawn since Anonymous is based on references that do not constitute prior art for the subject application.

Accordingly, Applicant respectfully submits that amended independent claim 1 now stands allowable.

Dependent claims 2, 4, and 7-11 depend from independent claim 1 and are allowable by virtue of their dependency from allowable claim 1, as well as for the additional features that each recites.

Independent claim 13, as amended, recites a method comprising:

- publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof; and
- decrypting an encrypted message using a decryption key corresponding to the isogeny, wherein the decryption is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

The Office argues that Anonymous anticipates the subject matter of claim 13 (prior to the amendment to this claim). The Office also argues that claim 13 (prior to the amendment to this claim) is obvious over Futa in view of Boneh and over Futa in view of Katsura. Applicant respectfully disagrees. Nevertheless, without conceding the propriety of the rejection and in the interests of expediting allowance of the application, independent claim 13 is amended to recite that the

"isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof." Independent claim 13 is further amended to recite that "the decrypting is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing." Dependent claims 15, 17 and 18 are incorporated into claim 13 with this amendment.

The amendments to claim 11 are similar to claim 1 above. Consequently, for similar reasons to those stated above, claim 11 now stands allowable.

Dependent claims 14, 16 and 19-22 depend from independent claim 11 and are allowable by virtue of their dependency from allowable claim 11, as well as for the additional features that each recites.

Independent claim 23, as amended, recites a system comprising:

- a first processor;
- a first system memory coupled to the first processor, the first system memory storing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve;
- a second processor;
- a second system memory coupled to the second processor, the second system memory storing an encrypted message and a decryption key corresponding to the isogeny to decrypt the

encrypted message, wherein the decryption is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing,

- wherein the encrypted message is encrypted using an encryption key.

The Office argues that Futa and Anonymous anticipate the subject matter of claim 23 (prior to the amendment to this claim). Applicant respectfully disagrees. Nevertheless, without conceding the propriety of the rejection and in the interests of expediting allowance of the application, independent claim 23 is amended to recite that the "the decrypting is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing." Dependent claims 26 and 27 are incorporated into claim 23 with this amendment. With respect to "bilinear pairing", claim 23 is amended similar to claims 1 and 13 above. For reasons similar to those stated above, claim 23 now stands allowable.

Dependent claims 24 and 25 depend from independent claim 23 and are allowable by virtue of their dependency from allowable claim 23, as well as for the additional features that each recites.

Independent claim 28, as amended, recites one or more computer-readable media having instructions stored thereon that, when executed, direct a machine to perform acts comprising:

- publishing a public key corresponding to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve, wherein the isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof; and
- decrypting an encrypted message using a decryption key corresponding to the isogeny, wherein the decrypting is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing.

The Office argues that Futa and Anonymous anticipate the subject matter of claim 28 (prior to the amendment to this claim). Applicant respectfully disagrees. Nevertheless, without conceding the propriety of the rejection and in the interests of expediting allowance of the application, independent claim 28 is amended to recite that the "isogeny is generated using a technique selected from a group comprising complex multiplication generation, modular generation, linearly independent generation, and combinations thereof." Independent claim 1 is

further amended to recite that "the decrypting is performed by bilinear pairing and wherein the bilinear pairing is a pairing selected from a group comprising Weil pairing, Tate pairing, and square pairing." Dependent claims 30, 32 and 33 are incorporated into claim 28 with this amendment. The amendments to claim 28 are similar to those in the other independent claims and are allowable for reasons similar to those stated above. Accordingly, claim 28 now stands allowable.

Dependent claims 29, 31 and 34-39 depend from independent claim 28 and are allowable by virtue of their dependency from allowable claim 28, as well as for the additional features that each recites.

Conclusion

All of the pending claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, **Applicant respectfully requests a call to discuss any remaining issues**.

Respectfully Submitted,

Dated: August 18, 2008

By: /Dale G. Mohlenhoff/
Dale G. Mohlenhoff
Reg. No. 37,683
(509) 324-9256 ext. 238

Robert G. Hartman
Reg. No. 58,970
(509) 324-9256 ext. 265